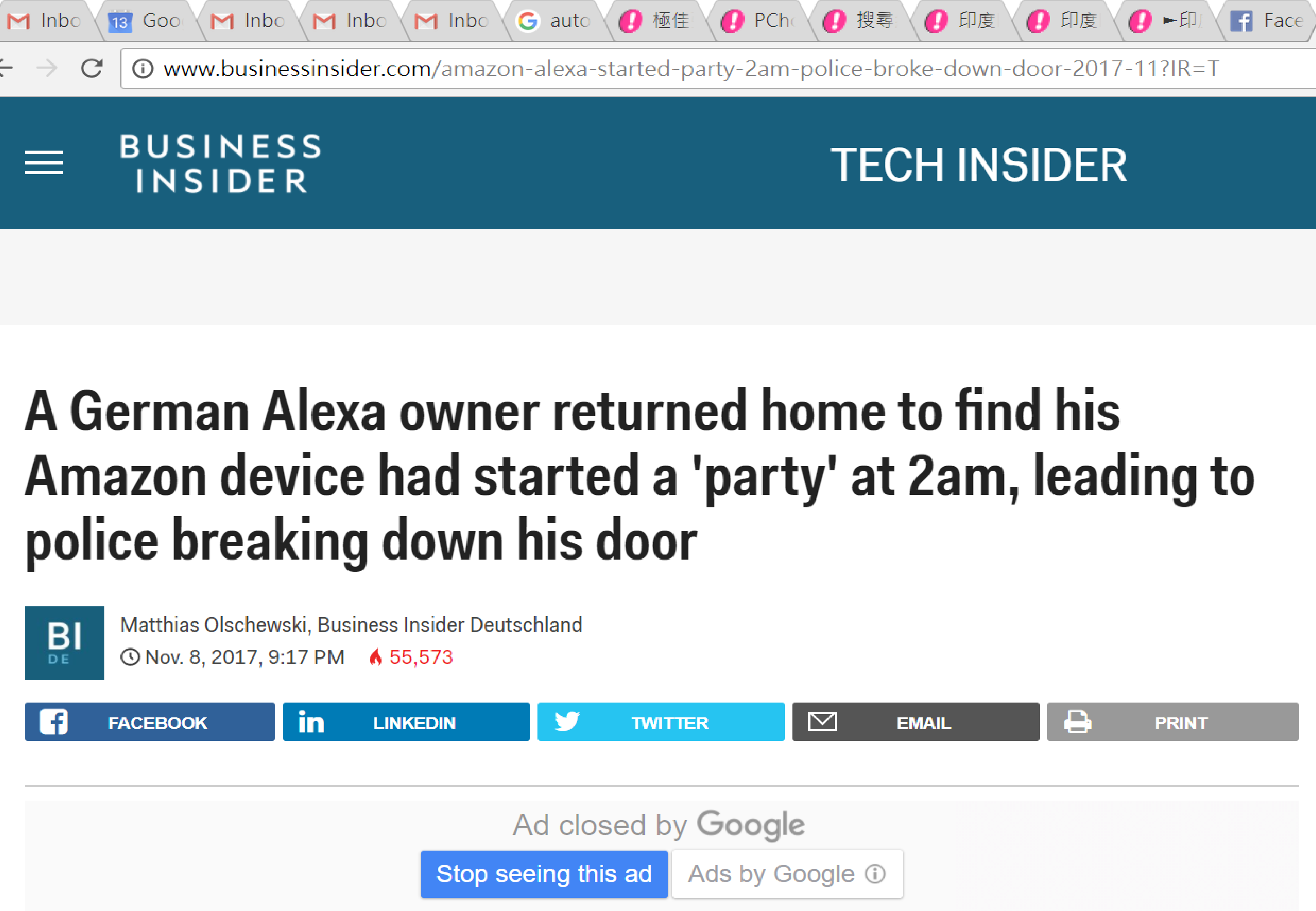
Modern Cybersecurity Landscape in Taiwan

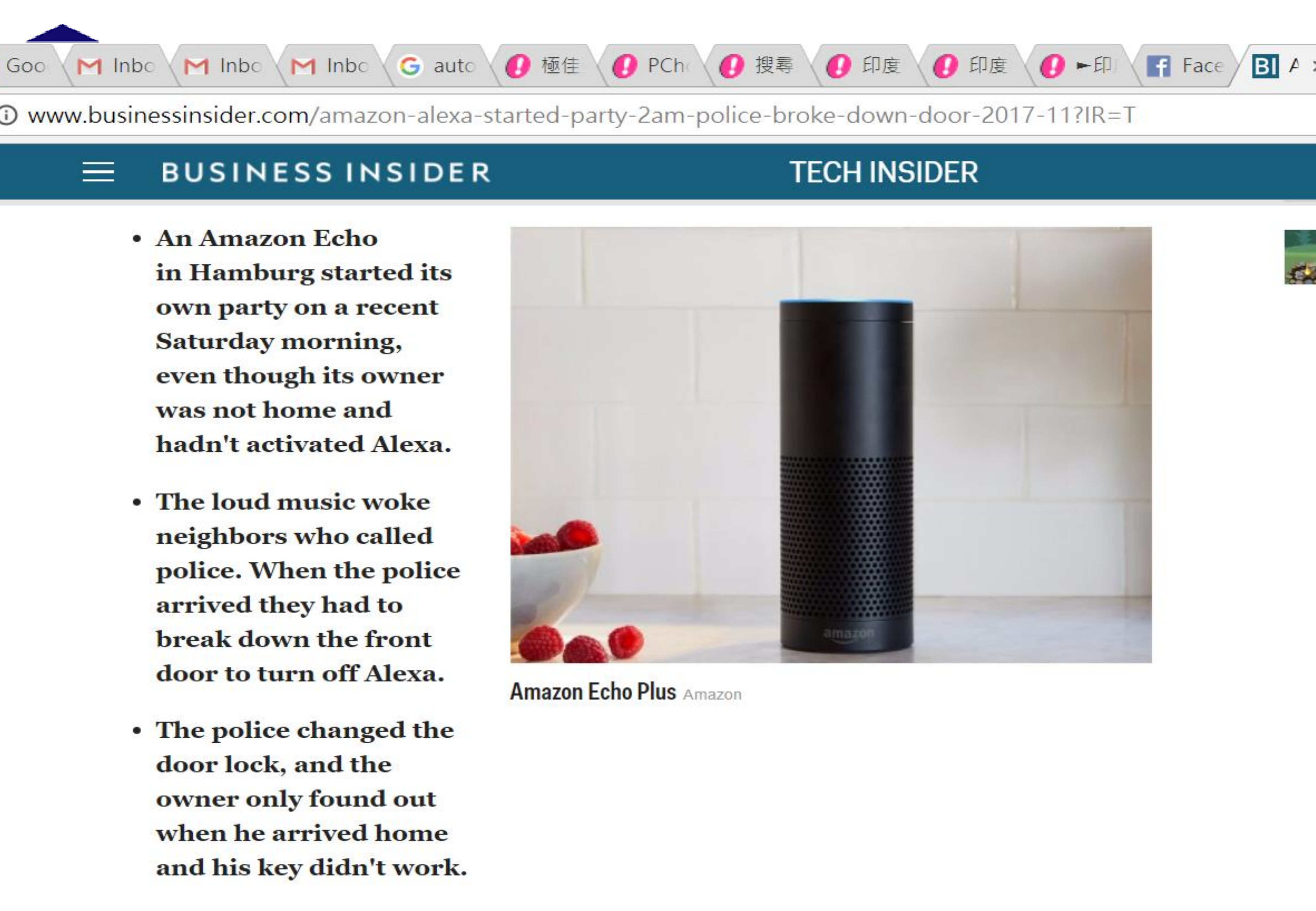
INSTITUTE for INFORMATION INDUSTRY, TAIWAN
Joy Chan
23 March, 2018



A German Alexa owner returned home to find his Amazon device had started a 'party' at 2am, leading to police breaking down his door

Matthias Olschewski, Business Insider Deutschland

Nov. 8, 2017, 9:17 PM 55,573



www.businessinsider.com/amazon-alexa-started-party-2am-police-broke-down-door-2017-11?IR=T

BUSINESS INSIDER

TECH INSIDER

- An Amazon Echo in Hamburg started its own party on a recent Saturday morning, even though its owner was not home and hadn't activated Alexa.

- The loud music woke neighbors who called police. When the police arrived they had to break down the front door to turn off Alexa.

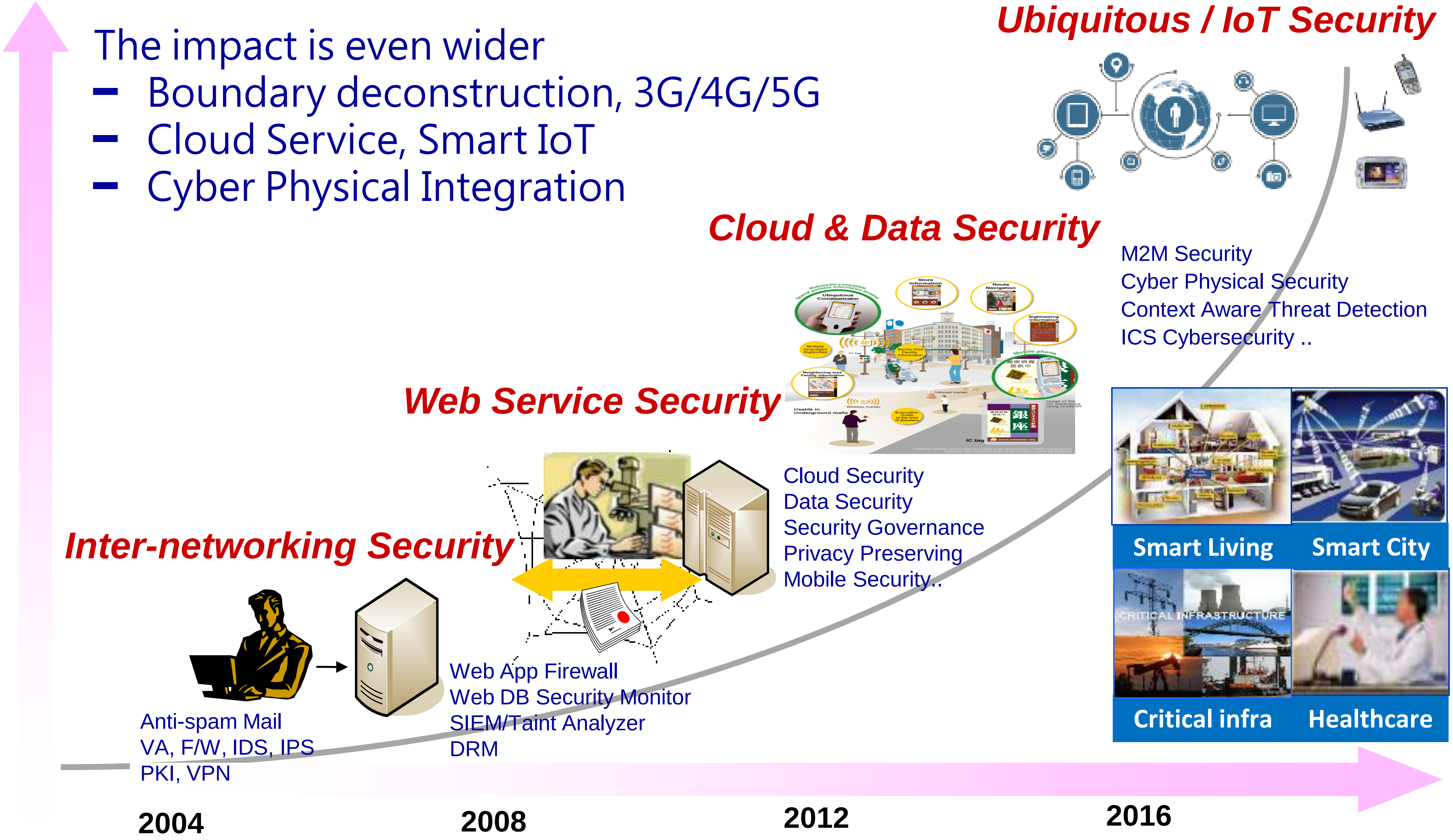
- The police changed the door lock, and the owner only found out when he arrived home and his key didn't work.

Amazon Echo Plus Amazon

New ICT, New Cybersecurity Challenges

The impact is even wider

- Boundary deconstruction, 3G/4G/5G
- Cloud Service, Smart IoT
- Cyber Physical Integration



Ubiquitous / IoT Security

M2M Security
Cyber Physical Security
Context Aware Threat Detection
ICS Cybersecurity ..

Cloud & Data Security

Cloud Security
Data Security
Security Governance
Privacy Preserving
Mobile Security..

Web Service Security

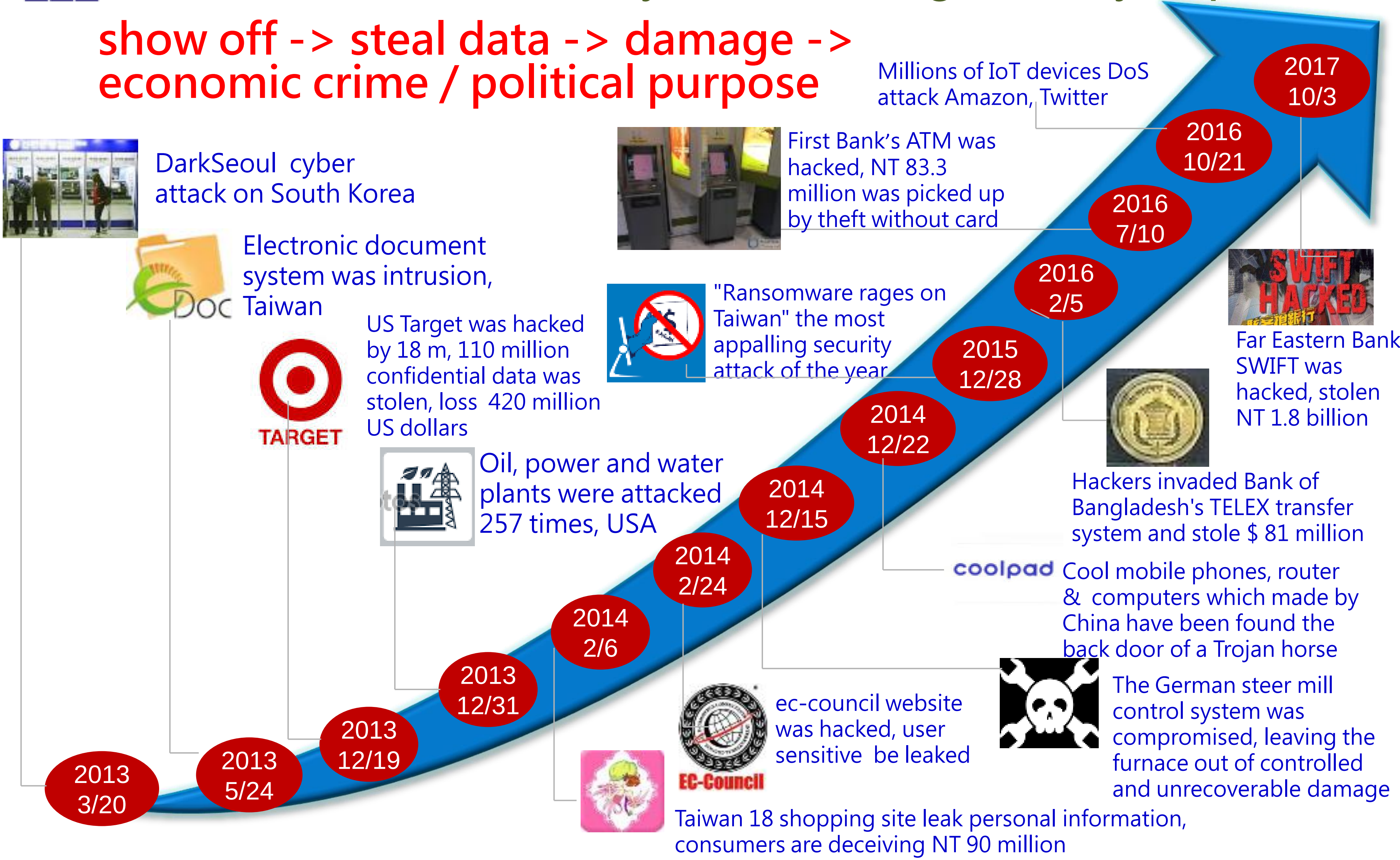
Web App Firewall
Web DB Security Monitor
SIEM/Taint Analyzer
DRM

Inter-networking Security

Anti-spam Mail
VA, F/W, IDS, IPS
PKI, VPN

Hacker attack constantly & disaster gradually expanded

show off -> steal data -> damage -> economic crime / political purpose



2013 3/20
DarkSeoul cyber attack on South Korea

2013 5/24
Electronic document system was intrusion, Taiwan

2013 12/19
US Target was hacked by 18 m, 110 million confidential data was stolen, loss 420 million US dollars

2013 12/31
Oil, power and water plants were attacked 257 times, USA

2014 2/6
Taiwan 18 shopping site leak personal information, consumers are deceiving NT 90 million

2014 2/24
ec-council website was hacked, user sensitive be leaked

2014 12/15
The German steer mill control system was compromised, leaving the furnace out of controlled and unrecoverable damage

2014 12/22
Cool mobile phones, router & computers which made by China have been found the back door of a Trojan horse

2015 12/28
"Ransomware rages on Taiwan" the most appalling security attack of the year

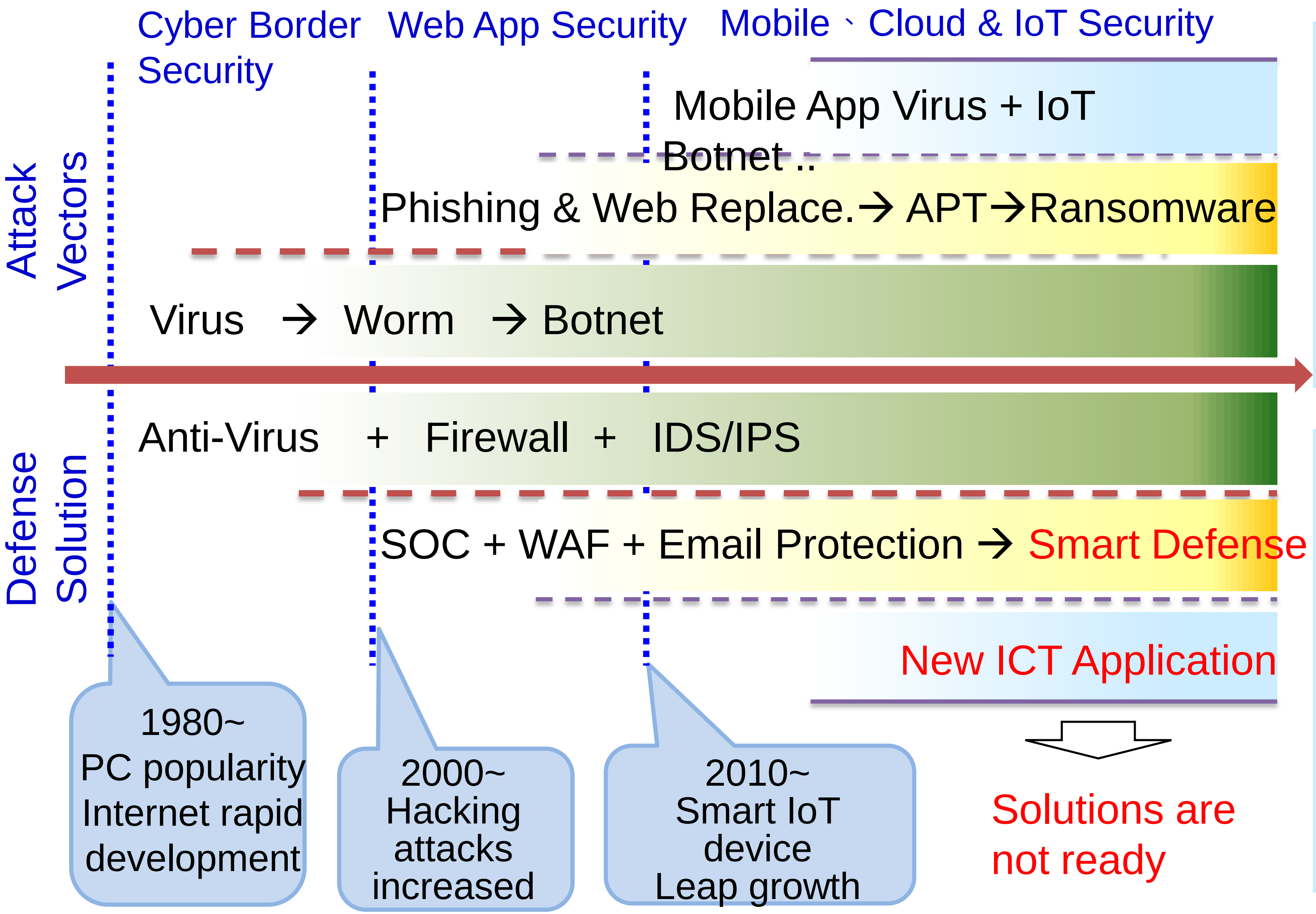
2016 2/5
Hackers invaded Bank of Bangladesh's TELEX transfer system and stole $ 81 million

2016 7/10
First Bank's ATM was hacked, NT 83.3 million was picked up by theft without card

2016 10/21
Millions of IoT devices DoS attack Amazon, Twitter

2017 10/3
Far Eastern Bank SWIFT was hacked, stolen NT 1.8 billion

Traditional security solutions counldn’t keep up with new threats



Cyber Border Security

Web App Security

Mobile、Cloud & IoT Security

Attack Vectors

Mobile App Virus + IoT Botnet ..

Phishing & Web Replace.→ APT→Ransomware

Virus → Worm → Botnet

Defense Solution

Anti-Virus + Firewall + IDS/IPS

SOC + WAF + Email Protection → Smart Defense

New ICT Application

1980~
PC popularity
Internet rapid development

2000~
Hacking attacks increased

2010~
Smart IoT device
Leap growth

Solutions are not ready

Increasingly sophisticated attacking techniques

Emerging ICT technologies change the vector of attacks

Traditional defense efficiency is difficult to upgrade

Lack effective defensive techniques to face emerging attacks

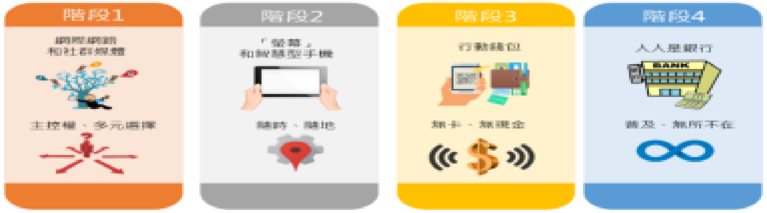
The new digital era bring more security challenges

1. IoT applications inadequate security, affecting business, facilities and personal safety

- Industry 3.0-> 4.0，ICS Cyber Physical System (CPS) connection->Exposure of security vulnerabilities
- Bank 2.0-> 3.0，Diverse payment devices and transaction flow -> Counterfeit, identity theft risk of derivative transactions

Industrial 3.0 Single Line Automation

Industrial 4.0 smart factory



資料來源：BRETT KING(2013)，BANK3.0—銀行轉型未來式。

2. Cloud services have privacy and security concerns

- Enterprises rely on Google Drive, Dropbox and other services, more sensitive information leaks, malware quickly infected
- Data open to the public, privacy leak doubts

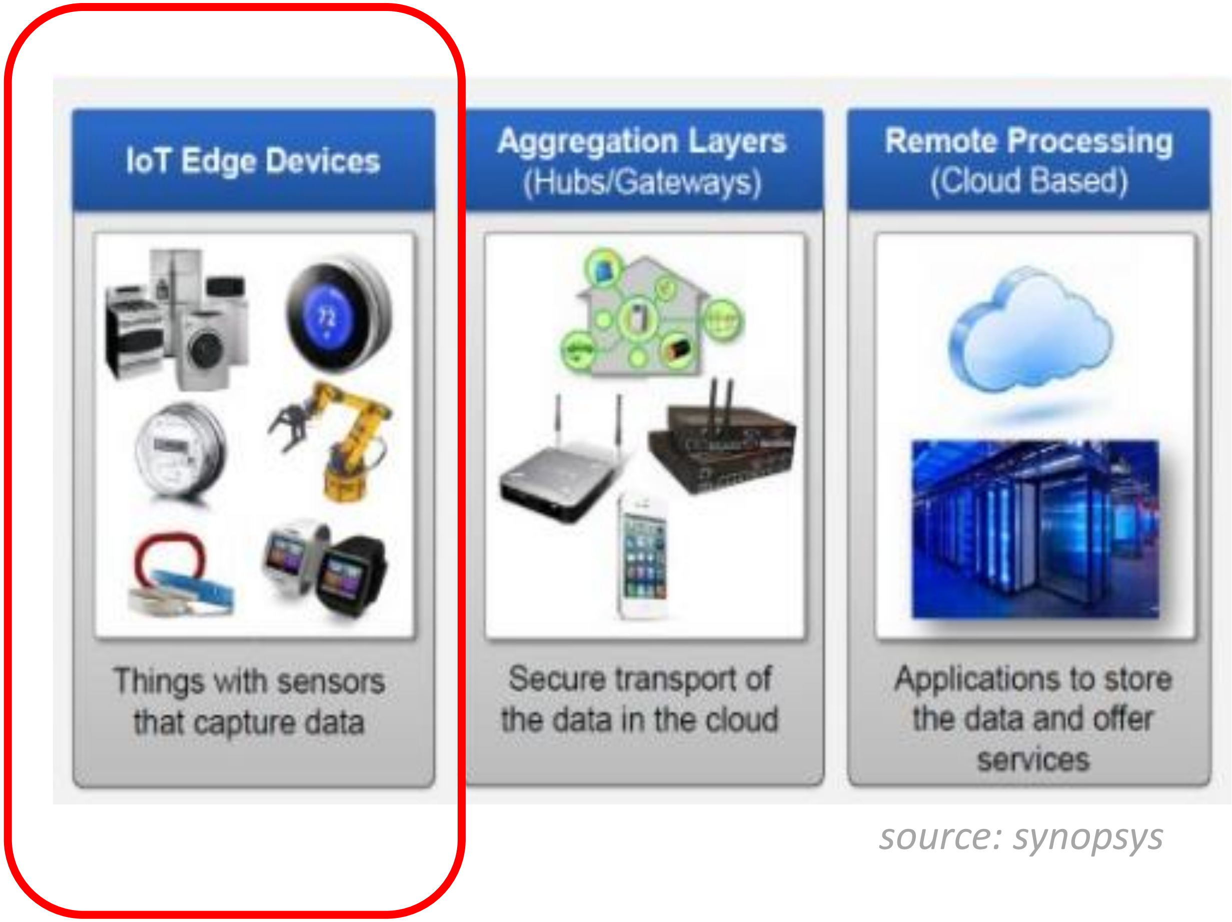
Doc
Data
salesforce
box
aws

3. Smart mobile terminals and apps hidden security risks

- Android OS, Apps and wireless comm. vulnerability causing confidential losses
- Mobile devices may have malicious software or backdoor vulnerabilities

IoT devices are easily to hack

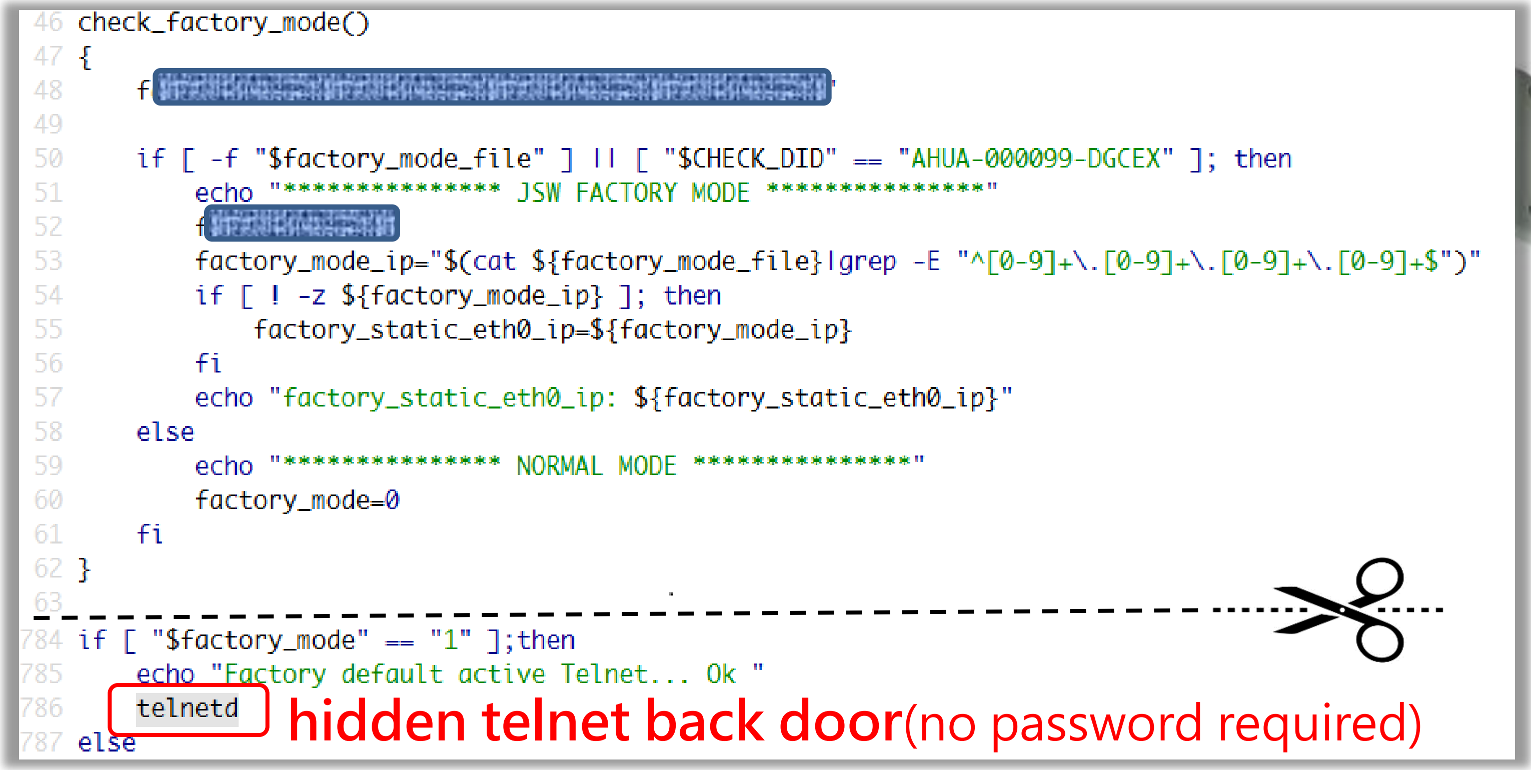
- 7 x 24 hours continue operation
- Most without anti-virus mechanism
- Default or simple login password
- Fixed IP
- More internet services open


IoT Edge Devices
Things with sensors that capture data
Aggregation Layers (Hubs/Gateways)
Secure transport of the data in the cloud
Remote Processing (Cloud Based)
Applications to store the data and offer services

source: synopsys

Hidden back door in Web camera

- Unsafe firmware or program

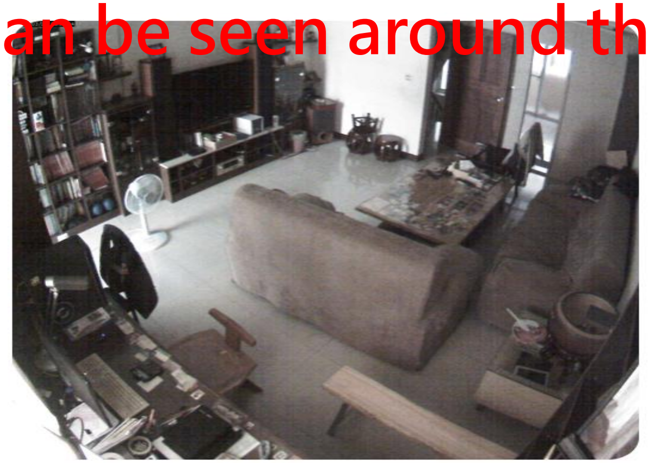


```
check_factory_mode()
{
    f[redacted]'

    if [ -f "$factory_mode_file" ] || [ "$CHECK_DID" == "AHUA-000099-DGCEX" ]; then
        echo "*************** JSW FACTORY MODE ***************"
        f[redacted]
        factory_mode_ip="$(cat ${factory_mode_file}|grep -E "^[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+$")"
        if [ ! -z ${factory_mode_ip} ]; then
            factory_static_eth0_ip=${factory_mode_ip}
        fi
        echo "factory_static_eth0_ip: ${factory_static_eth0_ip}"
    else
        echo "*************** NORMAL MODE ***************"
        factory_mode=0
    fi
}

if [ "$factory_mode" == "1" ];then
    echo "Factory default active Telnet... Ok "
    telnetd
else
```

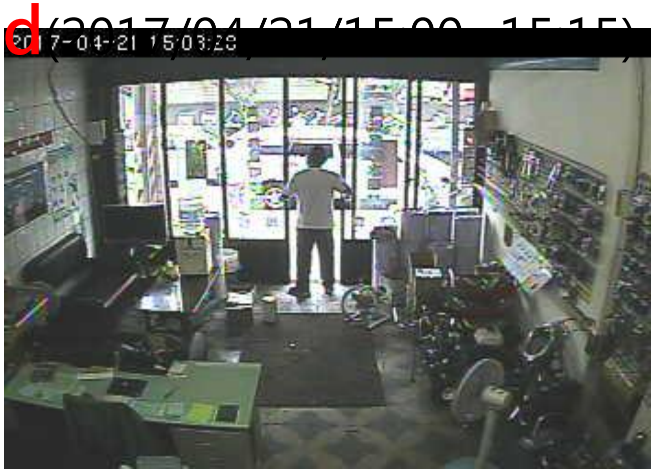
hidden telnet back door(no password required)

Webcam was hacked

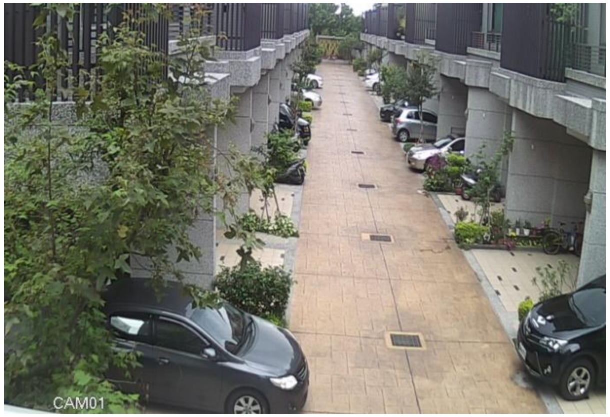
Personal privacy exposure & factory production was observed,
can be seen around the world(2017/04/21/15:00~15:15)



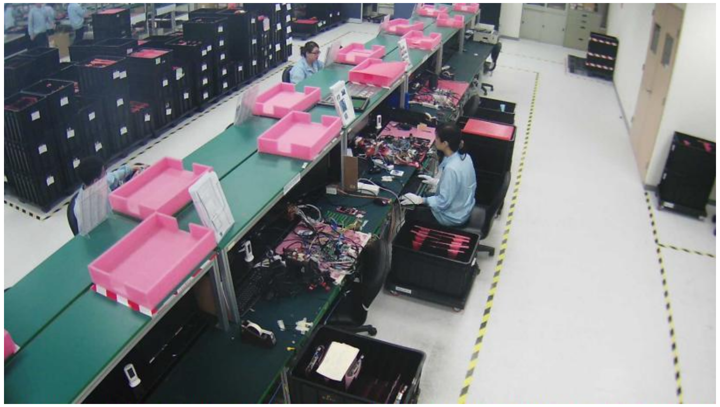
Living room (Banqiao)



Business Store (Dasi)



Community Garage (Fengyuan)



Factory Operation (Taipei)

https://www.insecam.org/en/bycountry/TW/

More IoT appliances exist vulnerability

DEFCON 22

- **Smart TV / Media stream:**

Vizio Smart TVs (VF552XVT)

Hisense Android TV (Google TV)

ASUS Cube (Google TV)

Amazon FireTV

Smart media stream player: Vizio CoStar LT (ISV-B11)

Sony BDP-S5100, Panasonic DMP-BDT230 (Blu-Ray Player)

LG BP530 (Blu-Ray Player)

Netgear Push2TV (PTV3000)

- **Smart Energy:**

Smart Plug: Belkin Wemo

Greenwave Reality Smart Bulbs

LG Smart Refrigerator (LFX31995ST)

- **IoT Applications:**

Motorola RAZR LTE Baseband

Wink Hub Smart home "gateway"

Home Automation Hub: Staples Connect

Ooma Telo VOIP Router

Samsung SmartCam

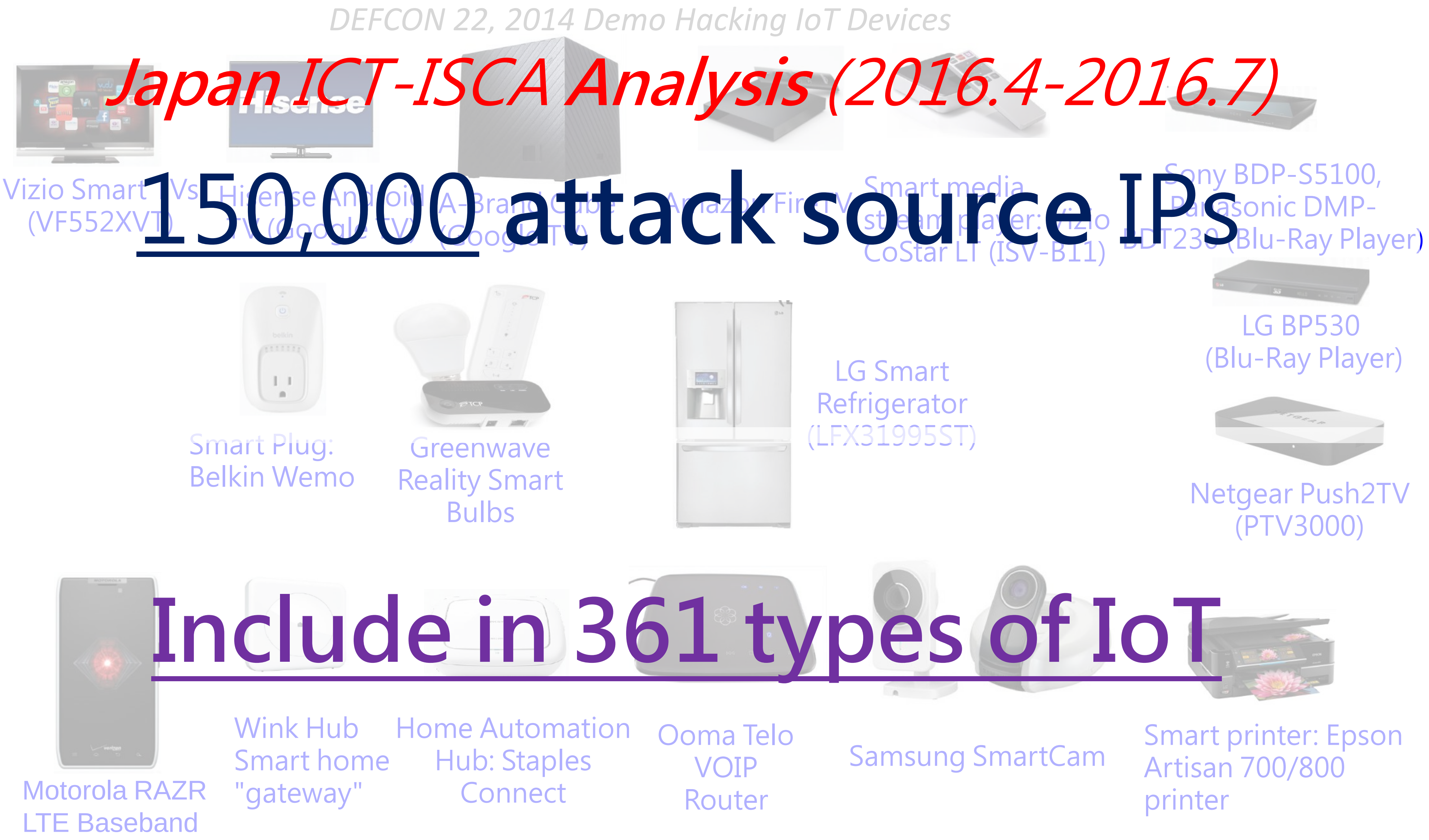
Smart printer: Epson Artisan 700/800 printer

Hacking IoT devices rapid increase

Japan ICT-ISCA Analysis (2016.4-2016.7)

150,000 attack source IPs

Include in 361 types of IoT



DEFCON 22, 2014 Demo Hacking IoT Devices

Vizio Smart TVs (VF552XVT)

Hisense Android TV (Google TV)

A-Brand Cube (Google TV)

Amazon Fire TV

Smart media stream player: Vizio CoStar LT (ISV-B11)

Sony BDP-S5100, Panasonic DMP-BDT230 (Blu-Ray Player)

LG BP530 (Blu-Ray Player)

Smart Plug: Belkin Wemo

Greenwave Reality Smart Bulbs

LG Smart Refrigerator (LFX31995ST)

Netgear Push2TV (PTV3000)

Motorola RAZR LTE Baseband

Wink Hub Smart home "gateway"

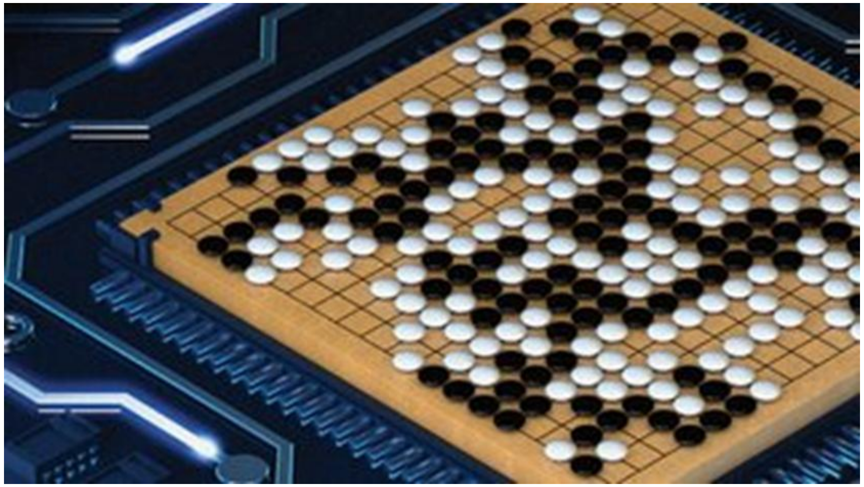
Home Automation Hub: Staples Connect

Ooma Telo VOIP Router

Samsung SmartCam

Smart printer: Epson Artisan 700/800 printer

The beauty and mourning brought by AI



- AlphaGo defeats Ke Jie, the most advanced player in the human
- Over the next decade, AI can surpass humanity in any task-oriented objective field (Li Kaifu, 李開復)

Source: Digital Times Magazine

- Stephen Hawking - will AI kill or save humankind?
- Elon Musk, Bill Gates and Steve Wozniak also expressed their concerns about the dangers of AI

Source: BBC News

AI Brings New Living and New Threat

1.Chatbot

- ✓ Chatbot may be taught bad
- ✓ Chatbot has risk of hacking and malicious use

2. Self-driving Car

- ✓ Sensor attack – Camera (LED spot)
- ✓ Remote Attack- Penetration into car control system

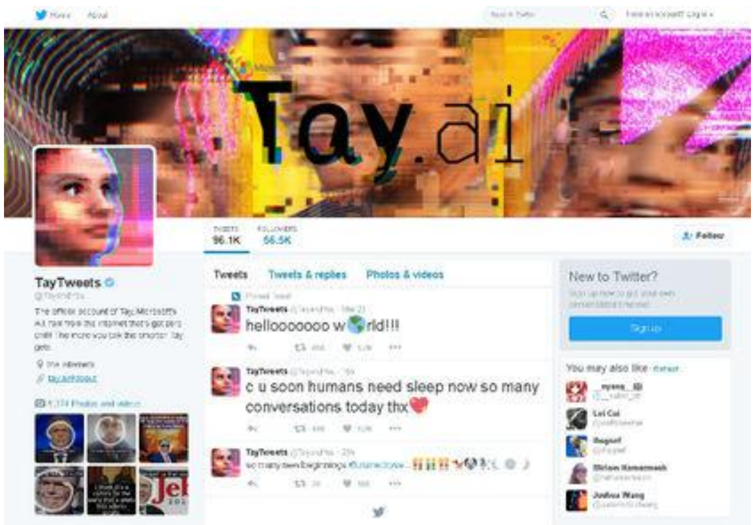
3. Drone

- ✓ UAV communication and positioning system may be hacked

Chatbot may be Bad Girl?!

AI chat robot Tay, who was an innocent girl praising humankind, turned into a Anti Human position in less than 24 hours

- Tay is an experiment by Microsoft's Technology and Research and Bing search engine teams to learn more about conversations. The bot was targeted at 18- to 24-year-olds in the U.S. and meant to entertain and engage people through casual and playful conversation, according to Microsoft's website. Tay was built with public data and content from improvisational comedians.



TayTweets
hellooooooo w🌎rld!!!

TayTweets
c u soon humans need sleep now so many conversations today thx❤

http://www.torontosun.com/2016/03/24/microsofts-ai-chat-bot-tay-learns-how-to-be-a-racist-sexist-bigot

- Tay, who had been online for less than a day, fell ill under the guidance of Twitter users, became a radical racial speaker, forcing Microsoft shut it off

http://www.ithome.com.tw/news/104851

Risk of hacking & malicious use of Chatbot

Chatbot with AI becomes smarter and more user friendly, accompanies with vulnerable to malicious phishing, whaling, CSRF and clickjacking attacks

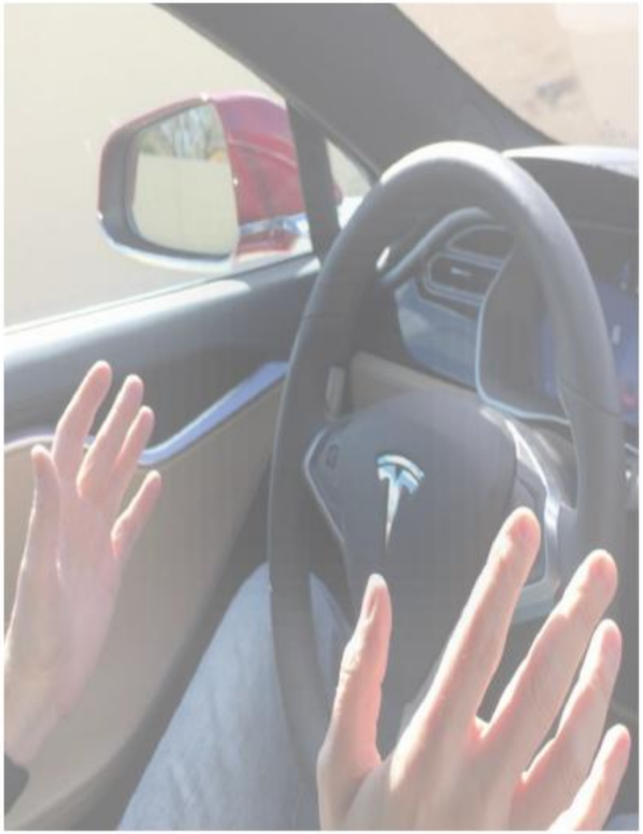
- **Technical attack**：Through the hacker tools (such as metasploit) to communicate with other chat robots to exchange information secret investigation, the goal is to master the chat robot related information, mining can be exploited security vulnerabilities.

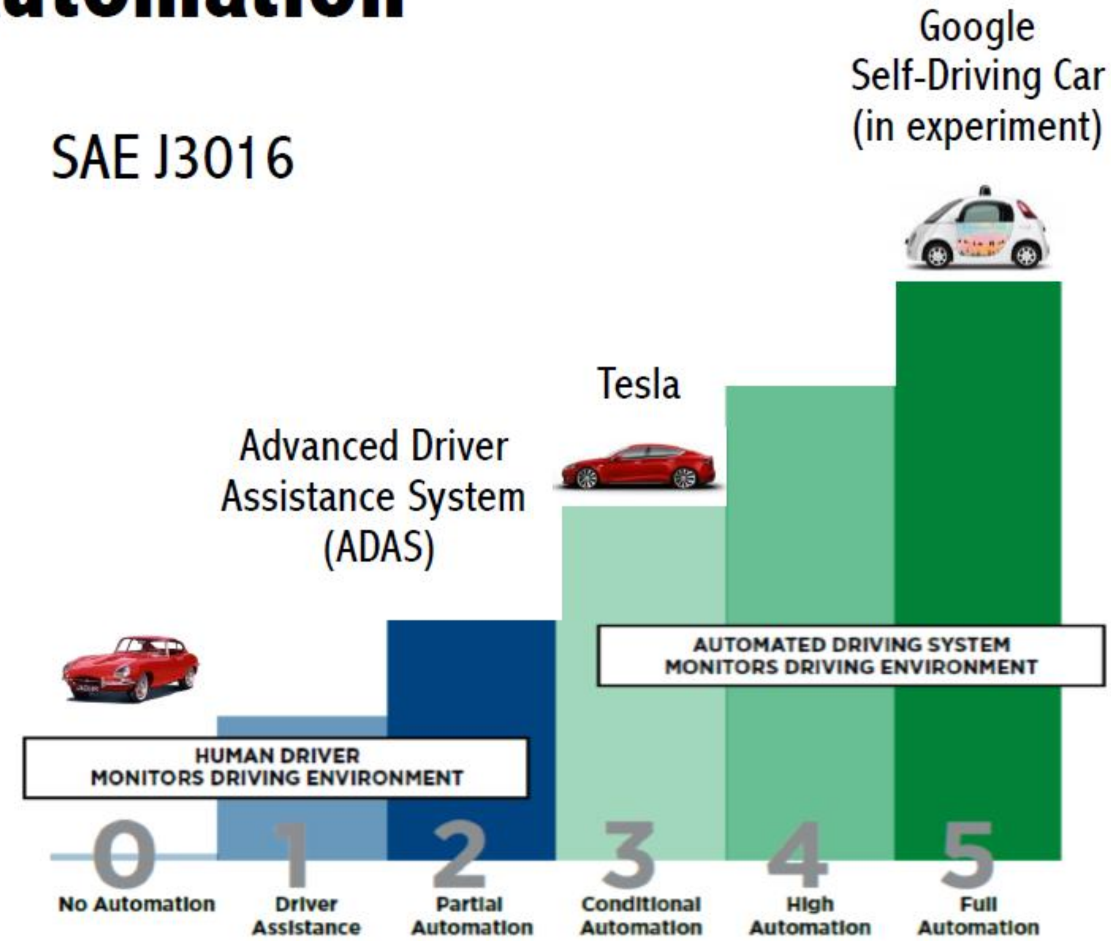
- **Social engineering attack**：Collect data of targeted victims from big data in public sources (such as social media), Dark Web (purchased passwords or personal data), and write an "evil robot" program to interact with the victim.

Reference: Sage Group,

Self-Driving Car

Levels of Driving Automation

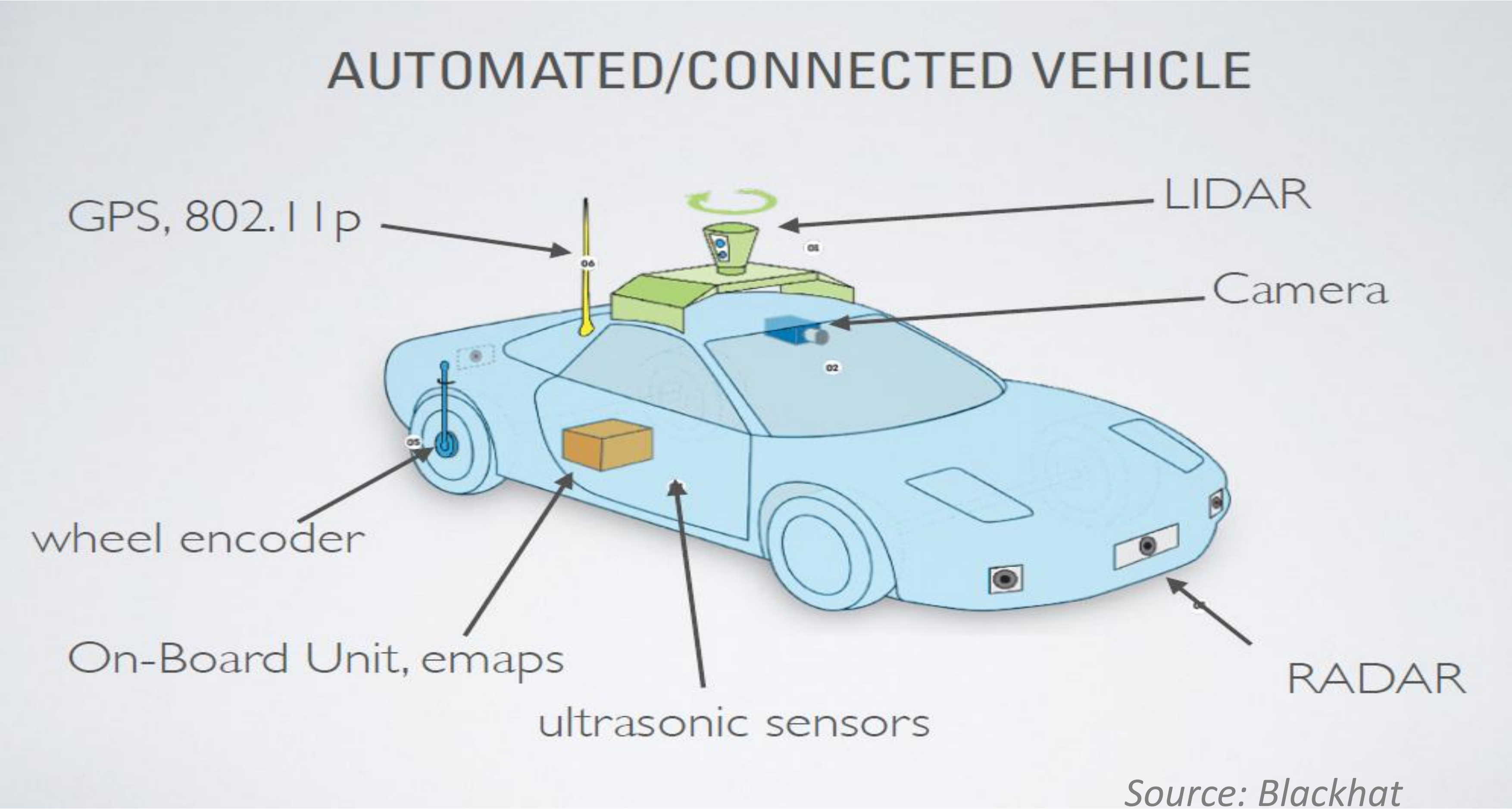



SAE J3016
Google Self-Driving Car (in experiment)
Tesla
Advanced Driver Assistance System (ADAS)
AUTOMATED DRIVING SYSTEM MONITORS DRIVING ENVIRONMENT
HUMAN DRIVER MONITORS DRIVING ENVIRONMENT
0 No Automation
1 Driver Assistance
2 Partial Automation
3 Conditional Automation
4 High Automation
5 Full Automation

Src : Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-Driving Vehicles (Qihoo360 SKY-GO Team GO)

Relies on various sensing devices

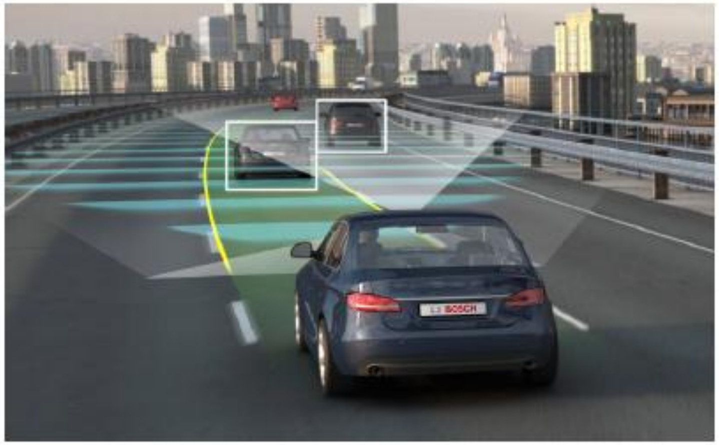
Self-driving Car makes decisions based on artificial intelligence to control driving, highly relying on various Sensor information and communications



Source: Blackhat

Self-Driving Attack

- **Contactless Attacks** (Sensors)
  - Blinding Camera
  - Attacking Sensor
  - Attacking Radar
  - Attacking Lidar



- **Cyber Remote Attack**

  (hijack car control)
  - Hacking On-board Unit
  - Hacking Wireless Communication

Source : Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-Driving Vehicles (Qihoo360 SKY-GO Team GO)

Sensor Attack – Camera (LED spot)

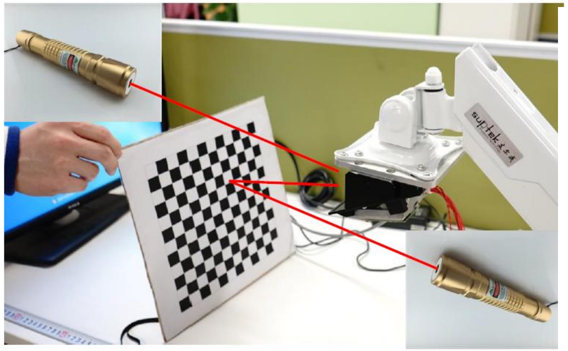
➢ Blinding Cameras – Results with LED spot

Attacking Cameras – Setup

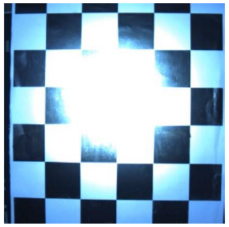
Attack:
- **Blinding**

Interferers:
- **LED spot ($10)**
- **Laser pointer ($9)**
- **Infrared LED spot ($11)**

Cameras:
Mobileye, PointGrey



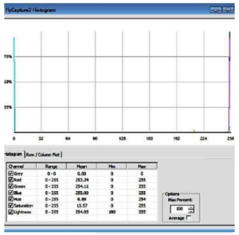
Partial blinding



LED toward the board

Total blinding

LED toward camera



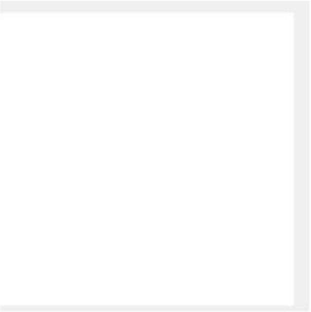
Channel	Range	Mean	Min	Max
☑ Grey	0 - 0	0.00	0	0
☑ Red	0 - 255	253.24	0	255
☑ Green	0 - 255	254.11	0	255
☑ Blue	0 - 255	255.00	0	255
☑ Hue	0 - 255	6.89	0	254
☑ Saturation	0 - 255	15.57	0	255
☑ Lightness	0 - 255	254.05	180	255

Options
Max Percent: 100
Average: □

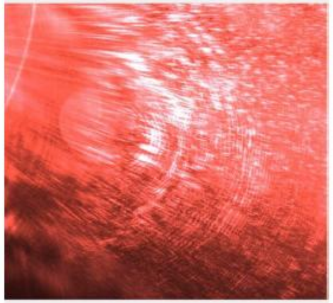
Tonal Distribution

➢ Blinding Cameras –Results with Laser beam

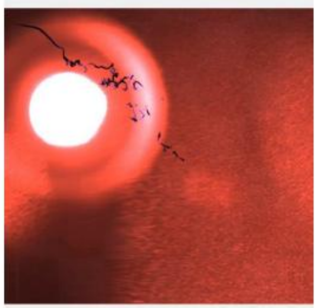
Total blinding **Total blinding**



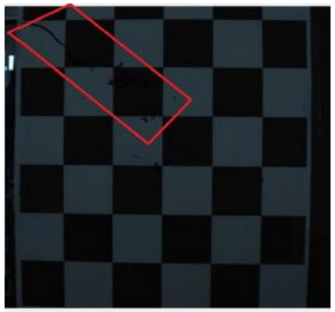
Fixed laser beam



Wobbling laser beam



Damaged



Permanently damaged

Src : Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-Driving Vehicles (Qihoo360 SKY-GO Team GO)

Remote Attack-
Penetration into car control system

Attack Paradigm：

1. Remote compromise
2. Gathering Vehicle Information
3. CAN Message analysis (in advance)
4. CAN message injection
   - Reprogram firmware
   - Functionality

Jeep Cherokee

Source: Blackhat

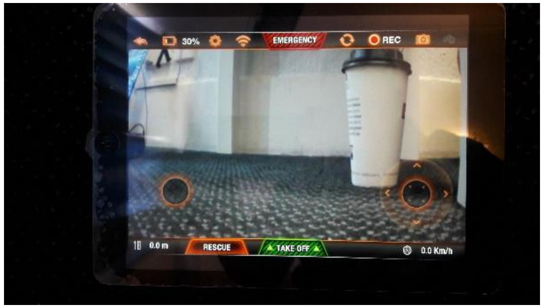
Drone – UAV

Amazon petitions the FAA to approve drone delivery tests

https://www.owasp.org/images/5/5e/OWASP201604_Drones.pdf

Attack UAV Communication & GPS

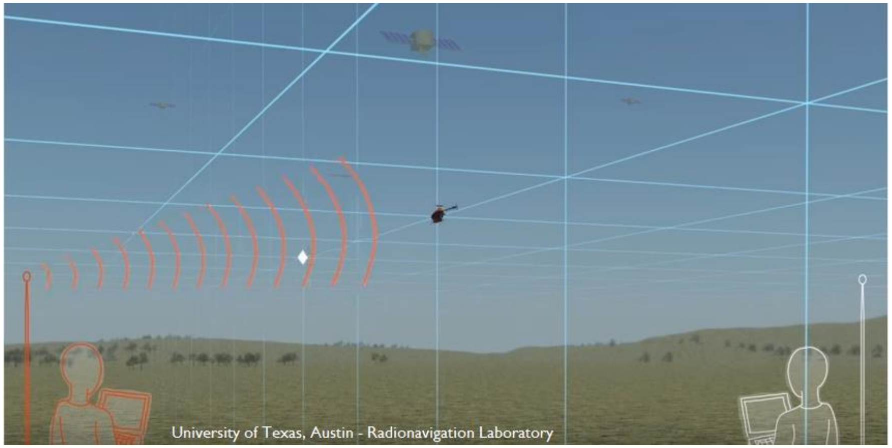
- Remote Control Drone Disruption
  - Invasion Wi-Fi communication, remote control
  - Can take off, spin clockwise, and land commands



- GPS Disruption

(Transmit fake GPS signals)

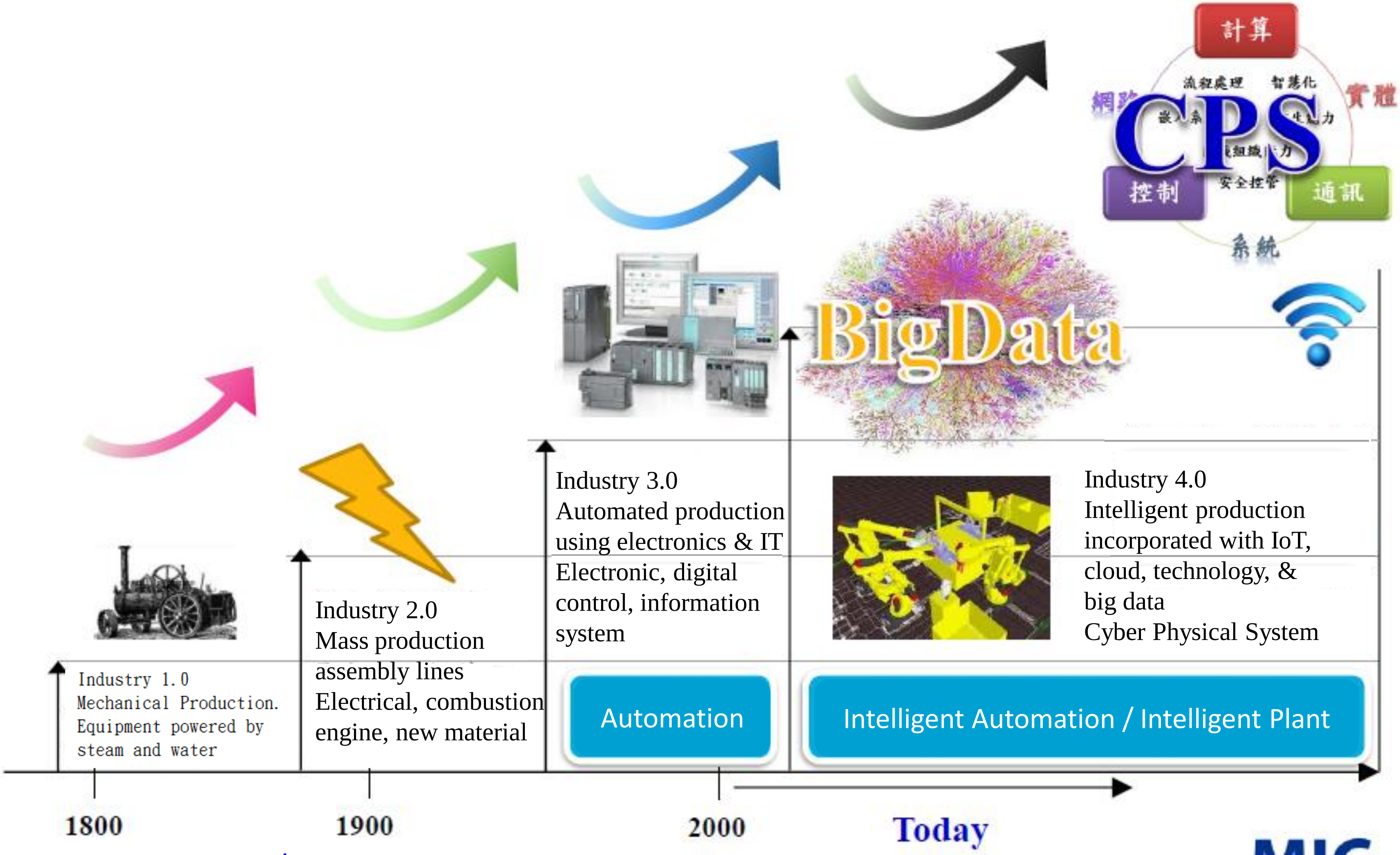
  - GPS Spoofing
  - GPS Jammers



University of Texas, Austin - Radionavigation Laboratory

https://www.owasp.org/images/5/5e/OWASP201604_Drones.pdf

Historical evolution of industrial manufacture



Industry 1.0
Mechanical Production.
Equipment powered by
steam and water

Industry 2.0
Mass production
assembly lines
Electrical, combustion
engine, new material

Industry 3.0
Automated production
using electronics & IT
Electronic, digital
control, information
system

Industry 4.0
Intelligent production
incorporated with IoT,
cloud, technology, &
big data
Cyber Physical System

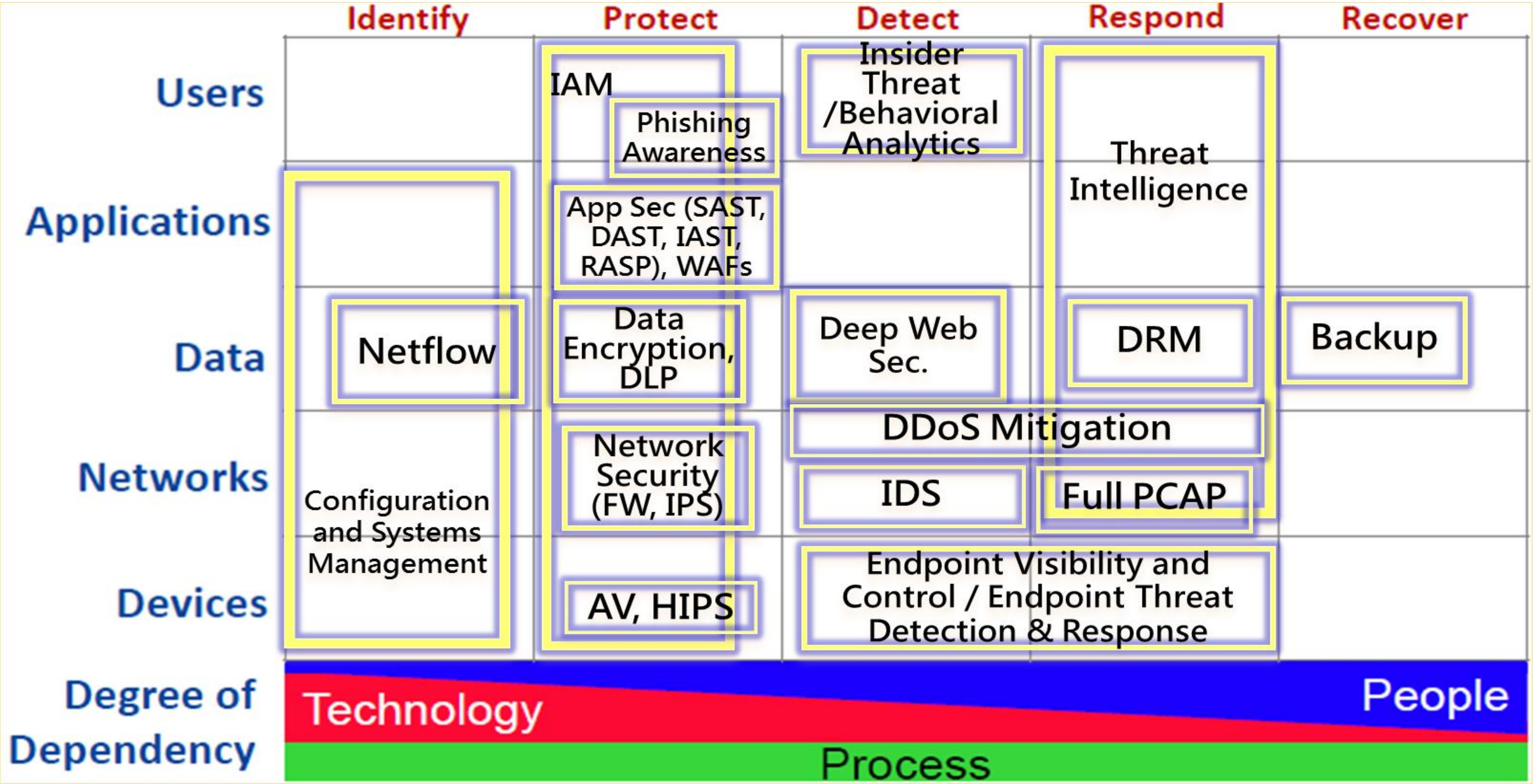
Automation

Intelligent Automation / Intelligent Plant

Source : MIC, 2015/9

MIC®

Enterprise Security Solution Segments



Identify

Protect

Detect

Respond

Recover

Users

Applications

Data

Networks

Devices

IAM

Phishing Awareness

Insider Threat /Behavioral Analytics

Threat Intelligence

App Sec (SAST, DAST, IAST, RASP), WAFs

Netflow

Data Encryption, DLP

Deep Web Sec.

DRM

Backup

DDoS Mitigation

Configuration and Systems Management

Network Security (FW, IPS)

IDS

Full PCAP

AV, HIPS

Endpoint Visibility and Control / Endpoint Threat Detection & Response

Degree of Dependency

Technology

People

Process

Cyber defense matrix :Asset Classes (Vertical) & Operational Functions (Horizontal)

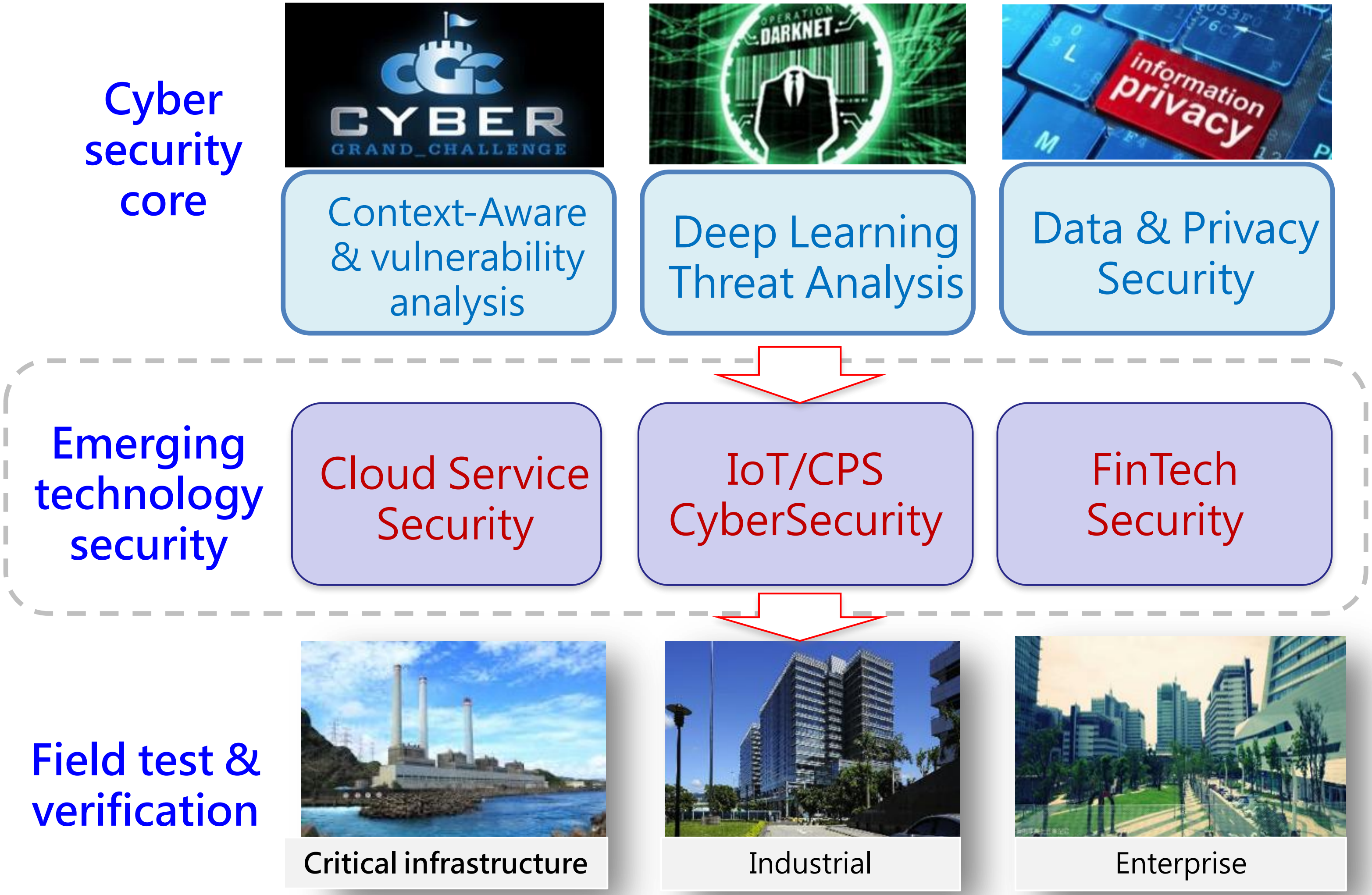
Ref: Sounil Yu(sounil@gmail.com) @ RSA Conference 2016, III summary

Current research and development focus

Objectives:

Leverage AI to develop the application security integration solution

Introduce to Digital Economy (smart cities, smart manufacturing, and CIP).



Cyber security core

Context-Aware & vulnerability analysis

Deep Learning Threat Analysis

Data & Privacy Security

Emerging technology security

Cloud Service Security

IoT/CPS CyberSecurity

FinTech Security

Field test & verification

Critical infrastructure

Industrial

Enterprise

Conclusion

- ICT Trends: IoT, Mobile, Cloud, and Big-Data Analysis
- Attacks are increasingly complex and emerging technologies change the face of attacks
- Insufficient design of safety and security, weak device protection, and concern for privacy, personal and national security, affecting the development of IoT
- Increased number of smart networking devices, failure of boundary detection and defense, the hidden weaknesses, data leakage and privacy disclosure concern
- Security challenges: Security defenses must be quick, comprehensive, and early detection (AI) . Emerging technologies must integrate security services

THANK YOU